Anomaly Detection Report

Model: autoencoder

Source File: synthetic_logs_1k.csv

Total Anomalies Found: 54

Anomaly #11 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

Log Details:

```
syslog_ts: Jan 28 08:10:08 host: servernameabc process: httpd[12345] ip1: 10.246.192.74 ip2: 0.1.0.1 session_id: 23565 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:08 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 547 response_time: 38 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as the size of the response is higher than usual for the given request.

Reason for Detection:

The anomaly detection model flagged this log entry due to the unusually high response size, which could indicate unauthorized extraction of data from the server.

Anomaly #21 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:10:16 host: servernameabc process: httpd[12345] ip1: 10.117.55.88 ip2: 0.1.0.1 session_id: 69500 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:16 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 559 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The anomaly features such as small size, negative values for Method_POST and Status, along with a high response time, suggest abnormal behavior that could be indicative of data exfiltration attempts.

Anomaly #42 | Severity: High | Type: Data Exfiltration (Score: 0.0012)

Log Details:

```
syslog_ts: Jan 28 08:10:30 host: servernameabc process: httpd[12345] ip1: 10.241.5.248 ip2: 0.1.0.1 session_id: 86438 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:30 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 213 response_time: 28 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as the POST method was used to send data out of the server.

Reason for Detection:

The negative anomaly score for Method_POST and the presence of a POST request with a relatively large size and response time

Anomaly Detection Report

suggest potential data exfiltration activity, which is a serious security concern.

Anomaly #44 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:10:32 host: servernameabc process: httpd[12345] ip1: 10.235.179.53 ip2: 0.1.0.1 session_id: 34867 domain: abc.example.net apache_ts: 28/Jan/2026:08:10:32 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 849 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The anomalous features 'Size' and 'Method_POST' suggest that a small amount of data was transferred using a POST request, which is commonly associated with data exfiltration techniques.

Anomaly #81 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:11:02 host: servernameabc process: httpd[12345] ip1: 10.245.60.247 ip2: 0.1.0.1 session_id: 99858 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:02 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 947 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information is being sent out from the server.

Reason for Detection:

The anomaly features Method_POST with a negative value and a larger Size value, suggesting a potential unauthorized data transfer through a POST request with a larger payload size.

Anomaly #107 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

Log Details:

```
syslog_ts: Jan 28 08:11:20 host: servernameabc process: httpd[12345] ip1: 10.225.144.131 ip2: 0.1.0.1 session_id: 35278 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:20 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 204 bytes: - response_time: 4762 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been sent out of the network.

Reason for Detection:

The anomaly features Method_POST and Size suggest that a POST request with non-standard size was made, which could indicate unauthorized data transfer.

Anomaly #134 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

Log Details:

Anomaly Detection Report

```
syslog_ts: Jan 28 08:11:35 host: servernameabc process: httpd[12345] ip1: 10.75.208.217 ip2: 0.1.0.1 session_id: 12518 domain: abc.example.net apache_ts: 28/Jan/2026:08:11:35 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 1190 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The anomaly features such as small size (0.0024) and a GET request for a specific resource could indicate an attempt to extract data from the server.

Anomaly #257 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:13:03 host: servernameabc process: httpd[12345] ip1: 10.200.252.25 ip2: 0.1.0.1 session_id: 55428 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:03 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 7650 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as there is a significant deviation in the Method_POST feature and the Status feature.

Reason for Detection:

The negative value for Method_POST and Status in the anomaly key features suggests abnormal behavior in the form of unauthorized data extraction through a POST request with a successful status code.

Anomaly #259 | Severity: High | Type: Data Exfiltration (Score: 0.0009)

Log Details:

```
syslog_ts: Jan 28 08:13:04 host: servernameabc process: httpd[12345] ip1: 10.20.26.46 ip2: 0.1.0.1 session_id: 64566 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:04 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 2321 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly in the server log indicates potential data exfiltration activity, as the POST request with a large response time and size could be indicative of sensitive data being sent out.

Reason for Detection:

The anomaly features Method_POST and Size being flagged, along with a high response time and large bytes transferred, suggest potential data exfiltration activity through the HTTP POST request.

Anomaly #264 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0004)

Log Details:

```
syslog_ts: Jan 28 08:13:06 host: servernameabc process: httpd[12345] ip1: 10.58.135.78 ip2: 0.1.0.1 session_id: 70795 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:06 +0530 request: GET /dashboard/stats HTTP/1.1 status: 404 bytes: - response_time: 4856 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

Anomaly Detection Report

The anomaly detected in the server log indicates a potential suspicious user agent accessing the server.

Reason for Detection:

The anomaly features such as status, size, and duration deviate significantly from normal patterns, suggesting a possible malicious intent from the user agent.

Anomaly #269 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0004)

```
Log Details:
syslog_ts: Jan 28 08:13:11 host: servernameabc process: httpd[12345] ip1: 10.206.67.89 ip2: 0.1.0.1 session_id: 26455 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:11 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 15144 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent attempting to access the server.

Reason for Detection:

The anomaly detection model flagged this log entry due to the unusual user agent string 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0', which may indicate a malicious actor attempting to disguise their identity.

Anomaly #277 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

```
Log Details:
syslog_ts: Jan 28 08:13:16 host: servernameabc process: httpd[12345] ip1: 10.191.228.102 ip2: 0.1.0.1 session_id: 45251 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:16 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 4278 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as the response time is unusually high for a 204 status code.

Reason for Detection:

The unusually high response time for a successful request, along with the presence of a user agent indicating a mobile device, suggests potential data exfiltration through a disguised HTTP request.

Anomaly #285 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0006)

```
Log Details:
syslog_ts: Jan 28 08:13:20 host: servernameabc process: httpd[12345] ip1: 10.136.136.134 ip2: 0.1.0.1 session_id: 82224 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:20 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 4604 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates a potential attack involving a suspicious user agent.

Reason for Detection:

The user agent 'Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36' is unusual and may be attempting to disguise malicious activity.

Anomaly Detection Report

Anomaly #321 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0006)

Log Details:

syslog_ts: Jan 28 08:13:49 host: servernameabc process: httpd[12345] ip1: 10.73.214.61 ip2: 0.1.0.1 session_id: 86773 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:49 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 4558 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The anomaly detected is likely due to a suspicious user agent string in the log entry.

Reason for Detection:

The user agent 'Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1' is uncommon and may indicate a potential security threat.

Anomaly #323 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0008)

Log Details:

syslog_ts: Jan 28 08:13:51 host: servernameabc process: httpd[12345] ip1: 10.208.167.153 ip2: 0.1.0.1 session_id: 71187 domain: abc.example.net apache_ts: 28/Jan/2026:08:13:51 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 368 response_time: 44 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent attempting to access the server.

Reason for Detection:

The user agent 'Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36' is not a typical user agent string and may indicate a malicious actor trying to disguise their identity.

Anomaly #361 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0007)

Log Details:

syslog_ts: Jan 28 08:14:21 host: servernameabc process: httpd[12345] ip1: 10.251.101.45 ip2: 0.1.0.1 session_id: 49270 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:21 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 338 response_time: 34 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The anomaly detected in the server log indicates a potential attack involving a suspicious user agent.

Reason for Detection:

The anomaly score for the user agent in the log is significant, suggesting that the request may be malicious or unauthorized.

Anomaly #367 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0006)

Log Details:

syslog_ts: Jan 28 08:14:27 host: servernameabc process: httpd[12345] ip1: 10.132.205.118 ip2: 0.1.0.1 session_id: 28263 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:27 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5424 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent accessing the server.

Anomaly Detection Report

Reason for Detection:

The anomaly detection model flagged this log entry due to the unusual user agent string 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0'. This could indicate a potential security threat or unauthorized access attempt.

Anomaly #404 | Severity: High | Type: Data Exfiltration (Score: 0.0010)

Log Details:

```
syslog_ts: Jan 28 08:14:51 host: servernameabc process: httpd[12345] ip1: 10.97.177.26 ip2: 0.1.0.1 session_id: 52318 domain: abc.example.net apache_ts: 28/Jan/2026:08:14:51 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 457 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as the response time is unusually high for a favicon request and the user agent is suspicious.

Reason for Detection:

The response time of 5 seconds for a small favicon request, along with a suspicious user agent string, suggests that data may be being exfiltrated from the server.

Anomaly #422 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

Log Details:

```
syslog_ts: Jan 28 08:15:02 host: servernameabc process: httpd[12345] ip1: 10.6.207.103 ip2: 0.1.0.1 session_id: 39308 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:02 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 204 bytes: - response_time: 4816 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The anomaly feature 'Method_POST' with a positive value suggests that a POST request was made to the server, which could indicate an attempt to send data out of the server. This, combined with the high response time and absence of response data ('bytes': '-'), raises suspicion of data exfiltration.

Anomaly #427 | Severity: High | Type: Data Exfiltration (Score: 0.0009)

Log Details:

```
syslog_ts: Jan 28 08:15:04 host: servernameabc process: httpd[12345] ip1: 10.48.91.12 ip2: 0.1.0.1 session_id: 56075 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:04 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 350 response_time: 48 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information is being extracted from the server.

Reason for Detection:

The anomaly features Method_GET and Size suggest that a GET request was made with a larger than usual response size, indicating potential data exfiltration activity.

Anomaly Detection Report

Anomaly #447 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

Log Details:

```
syslog_ts: Jan 28 08:15:18 host: servernameabc process: httpd[12345] ip1: 10.156.47.100 ip2: 0.1.0.1 session_id: 30478 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:18 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 4583 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information is being extracted from the server.

Reason for Detection:

The negative anomaly score for Method_POST and Status flags a potential data exfiltration attempt through a POST request with a successful status code, which is highly suspicious behavior.

Anomaly #451 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:15:19 host: servernameabc process: httpd[12345] ip1: 10.153.107.158 ip2: 0.1.0.1 session_id: 43830 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:19 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 204 bytes: - response_time: 955 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The anomaly features such as small size (0.0024) and a GET request for a specific resource (json2.js) with a high response time (955 ms) suggest potential data exfiltration activity.

Anomaly #489 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:15:48 host: servernameabc process: httpd[12345] ip1: 10.107.19.175 ip2: 0.1.0.1 session_id: 89514 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:48 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 743 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information is being extracted from the server.

Reason for Detection:

The anomaly features such as small size (0.0025) and a GET request for a specific image file could suggest an attempt to exfiltrate data in a covert manner.

Anomaly #497 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:15:52 host: servernameabc process: httpd[12345] ip1: 10.53.72.175 ip2: 0.1.0.1 session_id: 12455 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:52 +0530 request: GET /dashboard/stats HTTP/1.1 status: 200 bytes: 1384 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML,
```

like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been accessed and transferred out of the system.

Reason for Detection:

The anomaly features Method_GET and Status suggest that a GET request with a successful status code was used to retrieve data from the server, which could be indicative of data exfiltration attempts.

Anomaly #508 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0005)

Log Details:

syslog_ts: Jan 28 08:15:58 host: servernameabc process: httpd[12345] ip1: 10.144.244.84 ip2: 0.1.0.1 session_id: 68921 domain: abc.example.net apache_ts: 28/Jan/2026:08:15:58 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 441 response_time: 32 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The anomaly detected in the server log indicates a potential attack involving a suspicious user agent.

Reason for Detection:

The user agent 'Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36' is unusual and may be attempting to exploit vulnerabilities in the system.

Anomaly #520 | Severity: High | Type: Data Exfiltration (Score: 0.0006)

Log Details:

syslog_ts: Jan 28 08:16:08 host: servernameabc process: httpd[12345] ip1: 10.80.194.75 ip2: 0.1.0.1 session_id: 64382 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:08 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 1158 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The anomaly features Method_POST and Size suggest that a large amount of data was sent via a POST request, which is indicative of potential data exfiltration.

Anomaly #550 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

syslog_ts: Jan 28 08:16:28 host: servernameabc process: httpd[12345] ip1: 10.199.254.191 ip2: 0.1.0.1 session_id: 94089 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:28 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 842 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive data is being extracted from the server.

Reason for Detection:

Anomaly Detection Report

The anomaly features such as a very small size of response data (0.0024), along with a GET request for a specific resource, suggest that data may be exfiltrated through this request.

Anomaly #551 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

```
Log Details:
syslog_ts: Jan 28 08:16:30 host: servernameabc process: httpd[12345] ip1: 10.125.60.212 ip2: 0.1.0.1
session_id: 53887 domain: abc.example.net apache_ts: 28/Jan/2026:08:16:30 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 200 bytes: 5129 response_time: 5 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as the request method is GET and the status is 200, with a significant response time and large number of bytes transferred.

Reason for Detection:

The anomaly features Method_GET and Status being flagged suggest a potential data exfiltration attempt through a legitimate HTTP GET request, which could be used to extract sensitive information from the server.

Anomaly #618 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

```
Log Details:
syslog_ts: Jan 28 08:17:24 host: servernameabc process: httpd[12345] ip1: 10.231.61.239 ip2: 0.1.0.1
session_id: 30698 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:24 +0530 request: GET
/leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 732 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been transferred out of the network.

Reason for Detection:

The anomaly features such as small size, method POST, and status code 204 suggest abnormal data transfer behavior, which is commonly associated with data exfiltration attacks.

Anomaly #641 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0005)

```
Log Details:
syslog_ts: Jan 28 08:17:43 host: servernameabc process: httpd[12345] ip1: 10.17.80.115 ip2: 0.1.0.1
session_id: 28190 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:43 +0530 request: GET
/dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 1145 referer:
https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent accessing the server.

Reason for Detection:

The anomaly features indicate a small request size and a GET method, which are commonly associated with malicious activities such as data scraping or reconnaissance by a suspicious user agent.

Anomaly #644 | Severity: High | Type: Data Exfiltration (Score: 0.0006)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 28 08:17:46 host: servernameabc process: httpd[12345] ip1: 10.157.166.196 ip2: 0.1.0.1 session_id: 77376 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:46 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 19797 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information is being sent out from the server.

Reason for Detection:

The negative anomaly score for Method_POST and Status flags a potential data exfiltration attempt through a POST request with a successful status code, indicating the transfer of a large amount of data.

Anomaly #647 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

```
Log Details:
syslog_ts: Jan 28 08:17:48 host: servernameabc process: httpd[12345] ip1: 10.128.220.14 ip2: 0.1.0.1 session_id: 84044 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:48 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 15008 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive data is being sent out from the server.

Reason for Detection:

The negative anomaly score for Method_POST and Status, along with a high response time and large bytes transferred, suggest abnormal behavior associated with data exfiltration.

Anomaly #658 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0004)

```
Log Details:
syslog_ts: Jan 28 08:17:57 host: servernameabc process: httpd[12345] ip1: 10.0.246.37 ip2: 0.1.0.1 session_id: 35400 domain: abc.example.net apache_ts: 28/Jan/2026:08:17:57 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 530 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected in the server log suggests a potential attack involving a suspicious user agent.

Reason for Detection:

The anomaly features indicate a small request size, a negative value for Method_POST, and a negative value for Status, which are indicative of abnormal behavior possibly caused by a malicious user agent.

Anomaly #675 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

```
Log Details:
syslog_ts: Jan 28 08:18:08 host: servernameabc process: httpd[12345] ip1: 10.126.130.107 ip2: 0.1.0.1 session_id: 11791 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:08 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 204 bytes: - response_time: 1306 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as the size of the request is unusually small

compared to the response time.

Reason for Detection:

The anomaly features 'Size' and 'Method_GET' suggest that a small amount of data was requested using a GET method, which could be indicative of data exfiltration attempts.

Anomaly #680 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

Log Details:

```
syslog_ts: Jan 28 08:18:13 host: servernameabc process: httpd[12345] ip1: 10.122.170.156 ip2: 0.1.0.1 session_id: 36339 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:13 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 414 response_time: 31 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the system.

Reason for Detection:

The negative value for Method_POST feature and the unusually high response time for a small request size suggest abnormal behavior associated with data exfiltration.

Anomaly #705 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:18:33 host: servernameabc process: httpd[12345] ip1: 10.157.239.69 ip2: 0.1.0.1 session_id: 53557 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:33 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 1580 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The anomaly features Method_GET and Status suggest that a GET request with a successful status code was used to retrieve a potentially large amount of data, which could be indicative of data exfiltration.

Anomaly #709 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:18:35 host: servernameabc process: httpd[12345] ip1: 10.168.49.113 ip2: 0.1.0.1 session_id: 81537 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:35 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 10487 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The anomaly features Method_POST and Status suggest that a large amount of data (10487 bytes) was sent via a POST request with a successful status code (200), which is indicative of data exfiltration.

Anomaly Detection Report

Anomaly #710 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0004)

Log Details:

```
syslog_ts: Jan 28 08:18:36 host: servernameabc process: httpd[12345] ip1: 10.184.77.109 ip2: 0.1.0.1 session_id: 29599 domain: abc.example.net apache_ts: 28/Jan/2026:08:18:36 +0530 request: GET /favicon.ico HTTP/1.1 status: 204 bytes: - response_time: 4002 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent behavior.

Reason for Detection:

The user agent 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0' is uncommon and may indicate a malicious intent.

Anomaly #746 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:19:05 host: servernameabc process: httpd[12345] ip1: 10.241.8.57 ip2: 0.1.0.1 session_id: 44907 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:05 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 13319 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The negative anomaly score for Method_POST and Status, along with a high response time and large bytes transferred, suggest abnormal behavior that could be indicative of data exfiltration.

Anomaly #760 | Severity: High | Type: Data Exfiltration (Score: 0.0008)

Log Details:

```
syslog_ts: Jan 28 08:19:17 host: servernameabc process: httpd[12345] ip1: 10.15.214.128 ip2: 0.1.0.1 session_id: 25138 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:17 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 3483 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as there is a POST request with a high response time and a large number of bytes being transferred.

Reason for Detection:

The anomaly features Method_POST and Status suggest that a large amount of data was sent out of the server, which could indicate unauthorized data exfiltration.

Anomaly #792 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:19:38 host: servernameabc process: httpd[12345] ip1: 10.209.45.80 ip2: 0.1.0.1 session_id: 98630 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:38 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 307 response_time: 11 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

Anomaly Detection Report

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity through a POST request with a suspiciously low response time.

Reason for Detection:

The negative anomaly score for Method_POST and the low response time suggest that sensitive data may have been sent out of the server in a stealthy manner.

Anomaly #800 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0004)

Log Details:

```
syslog_ts: Jan 28 08:19:45 host: servernameabc process: httpd[12345] ip1: 10.197.130.57 ip2: 0.1.0.1 session_id: 45287 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:45 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 200 bytes: 16347 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0
```

LLM Analysis:

The anomaly detected in the server log suggests a potential suspicious user agent accessing the server.

Reason for Detection:

The anomaly detection model flagged this log entry due to the unusual user agent 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0', which may indicate a malicious actor attempting to access the server.

Anomaly #811 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0005)

Log Details:

```
syslog_ts: Jan 28 08:19:54 host: servernameabc process: httpd[12345] ip1: 10.11.112.24 ip2: 0.1.0.1 session_id: 30618 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:54 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 200 bytes: 18686 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent behavior.

Reason for Detection:

The user agent 'Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36' does not match typical user agent patterns, raising suspicion of a possible malicious intent.

Anomaly #816 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0006)

Log Details:

```
syslog_ts: Jan 28 08:19:57 host: servernameabc process: httpd[12345] ip1: 10.92.195.105 ip2: 0.1.0.1 session_id: 95107 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:57 +0530 request: GET /leave/appResources/css/Custom_font-awesome.css HTTP/1.1 status: 204 bytes: - response_time: 4656 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates a potential attack involving a suspicious user agent.

Reason for Detection:

The user agent 'Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36' is uncommon and may be attempting to disguise malicious activity.

Anomaly Detection Report

Anomaly #818 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0004)

Log Details:

```
syslog_ts: Jan 28 08:19:59 host: servernameabc process: httpd[12345] ip1: 10.200.211.83 ip2: 0.1.0.1 session_id: 84528 domain: abc.example.net apache_ts: 28/Jan/2026:08:19:59 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 3785 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent accessing the server.

Reason for Detection:

The user agent 'Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1' is uncommon and may indicate a malicious actor trying to access the server.

Anomaly #838 | Severity: High | Type: Data Exfiltration (Score: 0.0006)

Log Details:

```
syslog_ts: Jan 28 08:20:13 host: servernameabc process: httpd[12345] ip1: 10.84.4.161 ip2: 0.1.0.1 session_id: 77868 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:13 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5693 response_time: 5 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly in the server log indicates potential data exfiltration activity, where sensitive information is being sent out from the server.

Reason for Detection:

The negative anomaly score for Method_POST and Status suggests unusual behavior in sending data via POST method with a successful response, which could indicate data exfiltration.

Anomaly #870 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0006)

Log Details:

```
syslog_ts: Jan 28 08:20:39 host: servernameabc process: httpd[12345] ip1: 10.86.136.52 ip2: 0.1.0.1 session_id: 99004 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:39 +0530 request: GET /timesheet/resources/lib/js/json2.js HTTP/1.1 status: 204 bytes: - response_time: 4638 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected is likely due to a suspicious user agent string in the log entry.

Reason for Detection:

The user agent 'Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1' is unusual and may indicate a potential security threat.

Anomaly #890 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0012)

Log Details:

```
syslog_ts: Jan 28 08:20:53 host: servernameabc process: httpd[12345] ip1: 10.46.110.85 ip2: 0.1.0.1 session_id: 26195 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:53 +0530 request: GET /favicon.ico HTTP/1.1 status: 200 bytes: 224 response_time: 39 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

Anomaly Detection Report

LLM Analysis:

The anomaly detected in the server log indicates a potential attack involving a suspicious user agent.

Reason for Detection:

The user agent 'Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1' is unusual and could be indicative of a malicious actor attempting to disguise their identity.

Anomaly #902 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

```
Log Details:
syslog_ts: Jan 28 08:20:59 host: servernameabc process: httpd[12345] ip1: 10.229.108.87 ip2: 0.1.0.1 session_id: 15291 domain: abc.example.net apache_ts: 28/Jan/2026:08:20:59 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 5021 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The negative anomaly score for Method_POST and Status, along with a high response time for a relatively small request size, suggests abnormal behavior that could be indicative of data exfiltration.

Anomaly #905 | Severity: High | Type: Data Exfiltration (Score: 0.0005)

```
Log Details:
syslog_ts: Jan 28 08:21:02 host: servernameabc process: httpd[12345] ip1: 10.86.136.78 ip2: 0.1.0.1 session_id: 95078 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:02 +0530 request: GET /leave/appResources/images/lerf_default.png HTTP/1.1 status: 204 bytes: - response_time: 4450 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Mobile Safari/537.36
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The anomaly features Method_GET and Size suggest that a large amount of data was requested and potentially transferred out of the server, indicating a data exfiltration attempt.

Anomaly #960 | Severity: High | Type: Data Exfiltration (Score: 0.0010)

```
Log Details:
syslog_ts: Jan 28 08:21:45 host: servernameabc process: httpd[12345] ip1: 10.52.177.185 ip2: 0.1.0.1 session_id: 41070 domain: abc.example.net apache_ts: 28/Jan/2026:08:21:45 +0530 request: POST /leaverest/rest/lwpBatch HTTP/1.1 status: 200 bytes: 255 response_time: 18 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as the POST method was used to send data out of the server.

Reason for Detection:

The negative value of Method_POST feature and the size of the data being sent (255 bytes) suggest a potential data exfiltration attempt, which is a critical security concern.

Anomaly Detection Report

Anomaly #981 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0007)

Log Details:

syslog_ts: Jan 28 08:22:00 host: servernameabc process: httpd[12345] ip1: 10.27.251.198 ip2: 0.1.0.1 session_id: 76740 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:00 +0530 request: GET /dashboard/stats HTTP/1.1 status: 204 bytes: - response_time: 4810 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The anomaly detected in the server log indicates a potential attack involving a suspicious user agent.

Reason for Detection:

The user agent 'Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1' is unusual and may indicate an attempt to disguise malicious activity.

Anomaly #990 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

Log Details:

syslog_ts: Jan 28 08:22:09 host: servernameabc process: httpd[12345] ip1: 10.162.84.42 ip2: 0.1.0.1 session_id: 19009 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:09 +0530 request: POST /RightsWeb/myrights/rest/getNewCardBranch HTTP/1.1 status: 200 bytes: 4757 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 Edg/144.0.0.0

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information is being sent out from the server.

Reason for Detection:

The negative anomaly score for Method_POST and Status flags a potential data exfiltration attempt through a POST request with a successful status code, indicating unauthorized data transfer.

Anomaly #991 | Severity: High | Type: Data Exfiltration (Score: 0.0004)

Log Details:

syslog_ts: Jan 28 08:22:11 host: servernameabc process: httpd[12345] ip1: 10.211.9.6 ip2: 0.1.0.1 session_id: 97643 domain: abc.example.net apache_ts: 28/Jan/2026:08:22:11 +0530 request: POST /api/v1/auth/login HTTP/1.1 status: 200 bytes: 4308 response_time: 6 referer: https://abc.example.com/index.html user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0 Mobile/15E148 Safari/604.1

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the system.

Reason for Detection:

The negative anomaly score for the 'Method_POST' feature suggests unusual behavior for a POST request, which could indicate unauthorized data extraction or exfiltration.
